	Georgia Technology Authority		
Title:	**Email Security**		
PSG Number:	G-07-001.01	**Topical Area:** Security	
Document Type:	Guideline	**Pages:** 2	
Issue Date:	11/01/06	**Effective Date:**	09/01/07
POC for Changes:	GTA Information Technology Planning Office		
Synopsis:	To communicate the State industry best practices for email system security practice.		

PURPOSE

The purpose of this guideline is to communicate the industry best practices for email system security practice. Given the diversity in size of agencies the following may not be applicable for all agencies and are therefore stated as guidelines.

GUIDELINE

The Platforms that house email systems must be maintained according to best security practices.

- Timely application of security patches
- All administrative passwords will be complex
  - ⊡ The use of both upper- and lower-case letters (case sensitivity), and inclusion of one or more numerical digits, inclusion of special characters.
- Unused services will be turned off where possible
- Proper location in a protected network zone
- Limit the number of people who have full email administrative rights

Personnel: Background checks will be preformed on any persons employed who will administer email or be in a situation to access email for other employees without their express consent. The background checks will be at least as thorough at the standard GBI background checks used by most agencies for email administrators.
Authorization: A written or digital authorization must be presented from an authorized individual for an email administrator to view other employee's mail unless they have been delegated access by the employee. All such accesses will be logged.
Authentication: Access to email must require authentication and passwords. In the event that the agency chooses not to participate in a state wide reduced sign-on system, the individual will have to sign-on to email with a separate set of credentials.
Removable Media: A documented chain of custody will be maintained for all removable media used in backing up email systems. Removable media will be password protected.

Encryption: A minimum of 128 bit encryption of removable media. A Key storage and archiving system will guarantee retrieval of all keys used for encryption.
Storage: Must have the capability of providing isolated storage on dedicated hardware or in dedicated storage space.
Accounting and Audit logging: The email system will employ logging capabilities to capture adequate and detailed log information. This log information will be accessible only to email administrators. This log information must be backed up and applicable retention policies employed.

TERMINOLOGY/DEFINITIONS

Electronic mail, abbreviated **e-mail** or **email**, is a method of composing, sending, storing, and receiving messages over electronic communication systems or Email Systems. The term e-mail applies both to the Internet e-mail system based on the Simple Mail Transfer Protocol (SMTP) and to intranet systems allowing users within one company or organization to send messages to each other.
Email Systems are software and hardware systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local email system that carries messages to users within an agency or office over a local area network (LAN) or an enterprise-wide e-mail system that carries messages to various users in various physical locations over a wide area network (WAN) e-mail system to an e-mail system that sends and receives messages around the world over the internet. Often the same e-mail system serves all three functions.
E-mail messages are electronic documents created and sent or received by a computer via an e-mail system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. E-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda and circular letters.
User Levels

Email Administrator is an individual who has rights to create, delete and alter the email environment for example allocate additional space for a user.
User is the individual who is utilizing the email services.

Distribution lists are used to group email addresses where a single entry on the To: line of an email can send the email to more than one person across Agencies or external on one's own Agency.
Public Distribution lists are distribution lists that are created by an email administrator and have broad application within or across agencies.
Private Distribution lists are distribution lists are created by an individual user and can be limited by the users rights to the email system.